AF

Docket No.: 1363-006 Patent

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| In re application of | : | |
| JOSEPH ANDREW MELLMER et al. | : | |
| Serial No.: 09/670,783 | : | Group Art Unit: 2166 |
| Filed: September 27, 2000 | : | Examiner: Woo, Isaac M. |

For: MANAGING DIGITAL IDENTITY INFORMATION

**RE-INSTITUTED APPEAL BRIEF Responsive to RE-OPENING OF PROSECUTION**

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Responsive to the re-opening of prosecution in an Office Action dated February 21, 2007, the Appellant hereby appeals the final rejection of claims 1, 3-58 and 90-101. A fee transmittal indicating payment of the Appeal Brief Fee in the amount of $500.00 accompanied the previously filed Appeal Brief according to 37 C.F.R. §41.20(b)(2). A Notice of Appeal and attendant Notice of Appeal fee, in the amount of $500.00 according to 37 C.F.R. §§41.20(b)(1), was earlier filed on June 29, 2006. It is believed no additional fees are due. To the extent fees are nonetheless due, the undersigned authorizes their deduction from Deposit Account No. 11-0978.

## I. Real Party in Interest

The real party in interest is Novell, Inc., a corporation of the State of Delaware, having a principal place of business at 1800 South Novell Place, Provo, Utah 84606.

## II. Related Appeals and Interferences

The Appellant knows of no other prior or pending appeals, interferences, or judicial proceedings, which may be related to, directly affect, or be directly affected by, or have a bearing on, the Board's decision in this Appeal.

## III. Status of Claims

All pending claims (1, 3-58 and 90-101) stand finally rejected under 35 U.S.C. §102(e) in view of O'Flaherty et al. U.S. Patent No. 6,275,824. Claims 2 and 59-89, on the other hand, have long ago been canceled. On appeal, the Appellant traverses the rejection of all pending claims. Claims 1, 90 and 98 are independent.

## IV. Status of Amendments

No amendment has been filed subsequent to the Office Action dated February 21, 2007 and all previous amendments have been entered. In fact, no amendment has been filed subsequent to the earlier Final Office Action dated May 2, 2006. The form of the claims for purposes of appeal are those presented in the Amendment and Request for Continued Examination (RCE) filed by the Appellant on September 6, 2005 (received by the Patent Office on September 12, 2005) and re-presented for consideration in a Response filed by the

Appellant on February 10, 2006 (received by the Patent Office on February 13, 2006). As required, a copy of the claims is included herewith in Appendix form with double-spacing format.

## V. Summary of Claimed Subject Matter

Claims 1, 3-58 and 90-101 are pending. Claims 1, 90 and 98 are independent. The concise explanation of the subject matter defined in each of the independent claims is found, as in previous briefs, on pages 5-10 below. It also refers to each claim limitation in bold followed by a parenthetical cite to page and line number(s) of the specification, including a cross-reference to element and Figure numbers. Preceding it is a concise summary of the invention in paragraph form on pages 3-5. The Appellant appreciates the voluminous nature of the specification, which consists of seventy-six pages of text, including an additional forty-four figures, and it is intended as a pinpoint discussion to help the members of the Board readily ascertain the scope of the claims. As such:

The present invention relates broadly to computers, especially server systems and storage media for managing and controlling personal, digital identity information of users. More particularly, the present invention contemplates a vault for storage of safes that, in turn, correspond with one or more user objects, each with one or more profiles. Access rights to these items, however, are apportioned to a system administrator to effectively manage the items (e.g., safes) in the vault while, at the same time, the profiles are accessed and administered exclusively by a user at the exclusion of the system administrator. In addition, the profiles are operable to be exchanged or shared with other users who, in turn, have their own profiles accessible and administered exclusively by themselves at the exclusion of the administrator. In this manner:

> tools and techniques [are provided] to manage digital (e.g., online or connectable) identity information to support policies and membership in communities. In various embodiments, it helps provide and maintain the integrity of relationships, and helps provide reliable information access, within a secured storage platform using an extensible schema. *Appellant's specification, p. 3, ll. 23-27.*

As identified in the background section of the specification, the foregoing is a needed solution to "reduce user tedium, to increase users' control over their private information, and to provide better ways to manage personal information according to the relationship of the parties involved." *Underlining added, Appellant's specification, p. 3, ll. 13-15.*

In general, computer system servers of the invention are found in operating environments 100, Figure 1, and include or not individual computers, networks, servers, etc. 106, 108, 110, 112, 114. They are configured with appropriate hardware, software, combinations, etc. that are linked variously in infrastructure, such as via the Internet 104, for example, including or not various networked operating systems. *Appellant's specification, p. 9, l. 30 - p. 10, l. 27.*

The vaults 202 relate to that which stores one or more safes 200 of one or more users as representatively seen in Figure 2. Alternatively known as "vault objects" or "safe objects," as implemented in computer operating environments, for example, the "Safe objects and Vault objects are container objects" for containing other items. *Appellant's specification, p. 4, ll. 11-12.* That is, the vault "can hold Safe objects and other Vault objects." *Appellant's specification, p. 4, l. 18.* The Safe object, on the other hand, "belongs to and is managed by a particular . . . user." *Appellant's specification, p. 4, l. 12-13.* Among other things, it corresponds to user objects 308 representatively seen in Figure 3. In turn, the user objects 308 contain one or more profiles 300 particular to that user, e.g., "My hobby profile," "my biking profile," etc. A profile itself "can contain other profiles, e.g., Profiles

302, 304, 306" and, "for a given user[,] may contain distinct pieces of identity data, or they may share certain pieces of data, e.g., a user's work phone number." *Appellant's Specification, p. 13, ll. 15-19.* Ultimately, the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." *Appellant's specification, p. 13, ll. 23-25.* Figure 4 representatively shows John sharing a profile with Carol by way of representative access and contact lists 400, 402 for Carol and John, respectively.

In independent claim 1, and consistent with Figures 1-4, for example, the below-quoted limitations of the claim, in **bold**, are representatively found in the specification at the parenthetical cite as follows:

1. **A computer server system for managing digital identity information** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27*), **comprising at least one processor in operable connection with a memory configured by a database** ("*the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . .*" *Appellant's specification p. 10, l. 31 - p. 11, l. 3; and relative to Novell Directory Services (NDS) under the heading "NDS Software," for example, "[o]ne can create NDS objects for . . . databases . . ." Appellant's specification, p. 15, l. 17*), **the database including a vault for storage of multiple user objects for multiple users** *(vault 202 stores safes 200 and safes 200 correspond to user objects 308, for example, Figures 2 and 3, Appellant's specification p. 13, ll. 10-15*), **the vault having access rights granted to a system administrator for management of the multiple user objects** (*in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As*

*indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28*), **each of the user objects having a corresponding safe object** (*in one embodiment, "illustrated in Figure 8, a Vault account 800 includes the user object 308 and the Safe 200. Conceptually, the user object 308 belongs to and is managed by the Vault host 510. The host 510 can set the policy on the user object 308, e.g., by limiting the resources the user consumes. . . . The Safe 200 belongs to and is administered by the user, under the policy (such as space restriction) set by the host 510." Appellant's specification, p. 21, l. 23-28*), **the safe object containing multiple different profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator** (*"The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17*), **each profile including digital identity information provided by the single one of the multiple users** (*"the summation of a person's personal data can be termed a 'digital identity.'" Appellant's specification p. 13, l. 1; "As there are many aspects of a person's real identity, there can also be many aspects of a . . . digital identity; these multiple aspects are called 'Profiles.'" Appellant's specification, p. 13., ll. 12-13*) **and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users** (*this architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." Appellant's specification, p. 13, ll. 23-25*), **the sharing occurring exclusively upon initiation by the single one of the multiple users** (*"In*

*Figure 4, [for example] user Carol gives user John access by identifying John in an access list 400 and John includes Carol in his contact list 402. Carol defines the Profile . . . and grant[s] appropriate rights to the access structure 400." Appellant's specification, p. 13, ll. 25-28*).

In independent claim 90, the below-quoted limitations of the claim, in **bold**, are representatively found in the specification at the parenthetical cite as follows:

90. **A computer server system for managing digital identity information** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27*), **comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities** ("*the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . .*" *Appellant's specification p. 10, l. 31 - p. 11, l. 3*), **the vault including an access protocol layer, an identity server layer and an identity manager layer** ("*The identity Vault 202 provides storage of, and controlled access to, the identity data. In one embodiment, the identity Vault 200 is defined in three layers as illustrated in Figure 7, namely, an access protocol layer 700, an identity server layer 702, and an identity manager layer 704.*" *Appellant's specification, p. 19, l. 30 - p. 20, l. 2*) **and having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users** (*in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by*

*setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28*), **the one or more safes of digital identities having multiple profiles each with access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators** (*The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17*), **the multiple profiles being shared amongst the end users at the exclusion of the one or more system administrators** (*the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." Appellant's specification, p. 13, ll. 23-25. Figure 4 representatively shows John sharing a profile with Carol by way of representative access and contact lists 400, 402 for Carol and John, respectively.*).

In independent claim 98, the below-quoted limitations of the claim, in **bold,** are representatively found in the specification at the parenthetical cite as follows:

98. **A configured computer-readable storage medium that manages digital identities** (*Figure 1 and Appellant's specification under heading "Systems Generally," p. 9, l. 30 - p. 10, l. 27; and the servers 112, 114 and clients 106 may be uniprocessor or multiprocessor machines . . . each including an addressable storage medium 120, such as a random access memory . . ." Appellant's specification p. 10, l. 31 - p. 11, l. 3*), **comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer** (*"The identity*

*Vault 202 provides storage of, and controlled access to, the identity data. In one embodiment, the identity Vault 200 is defined in three layers as illustrated in Figure 7, namely, an access protocol layer 700, an identity server layer 702, and an identity manager layer 704." Appellant's specification, p. 19, l. 30 - p. 20, l. 2)* **and having access rights granted to a system administrator for management of the safes of digital identity profiles** *(in one embodiment, "Figure 10 illustrates access control by an administrator 1000 and an end user 1002 . . . As indicated by an arrow 1004 from the administrator 1000 to the Safe Container 902, the administrator has full administrative rights to the Vault. As indicated, by an arrow 1006 from the administrator 1000 to the end user 1002, the administrator manages the user's account by setting space restrictions, login restrictions, and so on. Finally, as indicated by an arrow 1008 from the end user 1002 to the safe 904, end users have full access control over their respective safes." Appellant's specification, p. 25, ll. 21-28)*, **the one or more safes of digital identity profiles having access rights granted exclusively to one or more end users at locations remote from the vault** *(The user stores his or her identity information in this Safe object. By default, only the user has rights to the Safe object (and by extension the information contained therein), each user can set policies to determine access to his or her own information." Appellant's specification p. 4, 13-17; end users are remote from the vault in any of a variety of instances in Figure 1, for instance)*, **the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator** *(the architecture "provides ways for individuals (including private persons and/or companies, organizations, etc.) to voluntarily exchange their information by sharing a profile 300." A profile itself "can contain other profiles, e.g., Profiles 302, 304, 306" and, "for a given user[,] may contain distinct pieces of identity data, or they may share certain pieces of data, e.g., a user's work phone number." Appellant's Specification, p. 13, ll. 15-19. Appellant's specification, p. 13, ll. 23-25. Figure 4 representatively shows John*

*sharing a profile with Carol by way of representative contact lists 400, 402 for Carol and John, respectively.*).

## VI. Grounds of Rejection to be Reviewed on Appeal

A. The Board must determine whether claims 1, 3-8 and 90-101 are rendered anticipated under 35 U.S.C. §102(e) in view of O'Flaherty. In this regard, the Board must essentially determine: A) whether O'Flaherty teaches identity profiles in a safe, in turn, in a vault, with access to manage the vault extending to a system administrator while access and administration rights of the profiles extend ***exclusively*** to users ***at the exclusion of the system administrator***; B) whether O'Flaherty teaches the sharing of profiles "exclusively upon initiation" by one of the multiple users; and C) whether O'Flaherty has abstraction layers, such as an identity server layer, an access protocol layer and an identity manager layer thereby defining a vault, especially a vault for storing safes, in turn, storing profiles with access to manage the vault extending to a system administrator while access and administration rights of the profiles extend to users at the exclusion of the system administrator.

To the extent the Board's determination finds any of the above in favor of the Appellant, the entirety of the claims should be adjudicated patentable in view of the pending rejections. Also, it will be seen that the Examiner's finding of facts fall far short of establishing a prima facie rejection of anticipation.

B. While not a ground of rejection, the Appellant also requests the Board to review the administrative handling of this file by the Examiner. This matter had its original claims rejected as obvious over Chang 6,157,953 in view of Van Dyke 6,412,070. According to the Examiner, Chang included all the elements of the independent claims with the exception that Van Dyke (relative to claims 1-58) incorporated "having access rights granted

to a system administrator, operable to be shared with other users having' [sic] other profiles accessible and administered exclusively by the other users, the string occurring exclusively upon initiation by the user." *Underlining added, Page 4, 1st ¶, 4-19-05 Final Rejection.* As is clear, the Examiner issued a Final Rejection on an erroneous record built on non-existent claim limitations about "the string" of something. Although the Applicant sought clarity, an Advisory Action issued and reiterated the notion of "the string."

After filing an RCE, to meet various timing obligations and including further clarification regarding "the string," the Examiner completely abandoned the Chang and Van Dyke references in lieu of the earlier-cited Dean and French references. As it relates to the claims, they have never been amended other than to reflect the nature of interaction of multiple users with multiple profiles, etc. Since adding aspects of multiplicity to the claims, it seems the Examiner's prior searching should have remained relevant and the Dean and French references certainly should have already been of record from prior searches and/or applied. The Chang and Van Dyke references should have also certainly been applicable to the Examiner's prior line of reasoning. However, no explanation has ever been given regarding the abandonment of Chang and Van Dyke in favor of Dean and French. Despite repeated attempts to build an appropriate record regarding "the sharing" of profiles, and not "the string," nothing has ever been advanced by the Examiner. The Appellant does not mind a thorough prosecution by the Examiner, however, prosecution has progressed confusingly for reasons unbeknownst to the Appellant. Also, while the cost of prosecution is fairly expensive in modern times, the cost in this matter has progressed seemingly unfairly relative to a confusing record. As can be appreciated, the burden to continually fend off imprecise reasoning is overly costly in time, effort and money to both the Appellant and the Patent Office.

As it stands now, the Dean and French references have been abandoned entirely in favor of O'Flaherty. This occurred upon the re-opening of prosecution and after the filing

of an Appeal Brief and an Amended Appeal Brief responsive to a Notice of Non-Compliant Appeal Brief. It seems that the record should indicate a modicum of reasoning as to why Dean and French are no longer cited.

## VII. Argument

### A. The Appellant offers the following preliminary remarks in consideration of its arguments.

#### 1. Brief Background of O'Flaherty U.S. Patent No. 6,275,824

O'Flaherty teaches a "database management system, for storing and retrieving data from a plurality of database tables wherein the data in the database tables is controllably accessible according to privacy parameters stored in the database table." *Col. 2, ll. 57-61.* A data warehousing system 100, as seen in Figure 1, includes a secure data warehouse 102 with an extended database 106 containing the privacy parameters of a client. By way of various "dataviews" in a suite 108, Figures 2A-3C for example, a requesting entity (e.g., third party or business applications 112 or 110) is furnished with certain of the privacy parameters, but only "as permitted by the [particular] database view provided." *Col. 4, ll. 40-41.* For security, the accessing or requesting of the privacy parameters can be logged and/or audited at 120, by an audit interface module 118. *E.g., Figures 1 and 4.*

In more detail, the privacy parameters of the extended database 106 of Figure 1 comprise, as seen in Figures 2A-3C, "a customer table 202, which is segmented into three portions: an identity information portion 204, a personal information portion 206, and a sensitive information portion 208." *Col. 7, ll. 12-15.* The dataviews, on the other hand, include: a standard view 260, for a routine DSS application requestor 110A; an anonymizing view 264, for an analytic application 110C or third party application requestor 112; an opt-

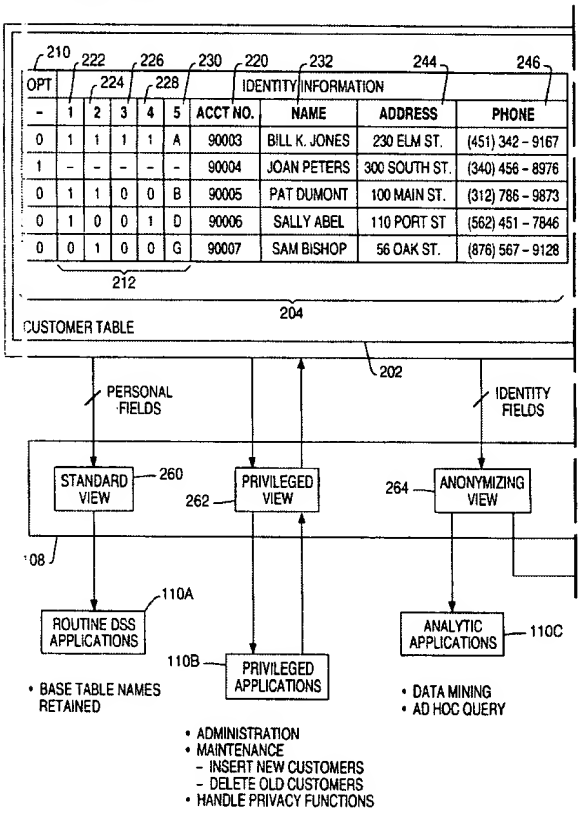
out view 266, for action applications 110D or third party application requestor 112; and a privileged view 262, for privileged applications 110B. In turn, each requestor in the form of a DSS application 110A, analytic application 110C, Action application 110D or a third party application 112 have certain "blocked" privacy parameters of the client. In Figures 2A-3C, and described at *col. 8, l. 16 et seq.*, the "personal fields" are blocked from the view of the DSS applications 110A, the "identity fields" are blocked from the view of the analytic applications 110C, and the "fields with active opt-out" are blocked from the view of the action applications. Both the "identity fields" and the "fields with active opt-out" are blocked from the view of third party applications 112. According to the specification, "[t]hese views limit visibility into the data in the customer table 202 in accordance with the values placed in the data control columns 212." *Col. 8, ll. 13-15.*

In the privileged view 262, however, nothing is blocked from view by the privileged applications 110B (including full access to "Administration," "Maintenance," and "Handle Privacy Functions"). *Figures 2A and 3A.* To the contrary, the **"privileged view 262 permits viewing, analysis, and alteration of all information [in customer table 202]."** *Emphasis added, col. 8, ll. 46-47.* Also, the privileged view 262 is supplied to "Class 'A' applications 110B, such as those required for administration and/or maintenance of the database (e.g. for inserting new customers, deleting ex-customers, handling address changes), and to those applications which handle privacy related functions (such as informing customers about personal information collected about them, changing/updating personal information, and applying 'Opt-in/Opt-out' controls)." *Col. 8, ll. 48-55.* Similarly, *col. 4, ll. 15-18*, teaches that "all accesses to data, ***(with the exception of data access for administrative purposes)*** is accomplished through dataviews." *Emphasis added.* In other words, those who perform system administration and maintenance on the extended database, e.g., system administrators, have access to the underlying privacy information of the clients.

## 2. Arrangement of O'Flaherty.

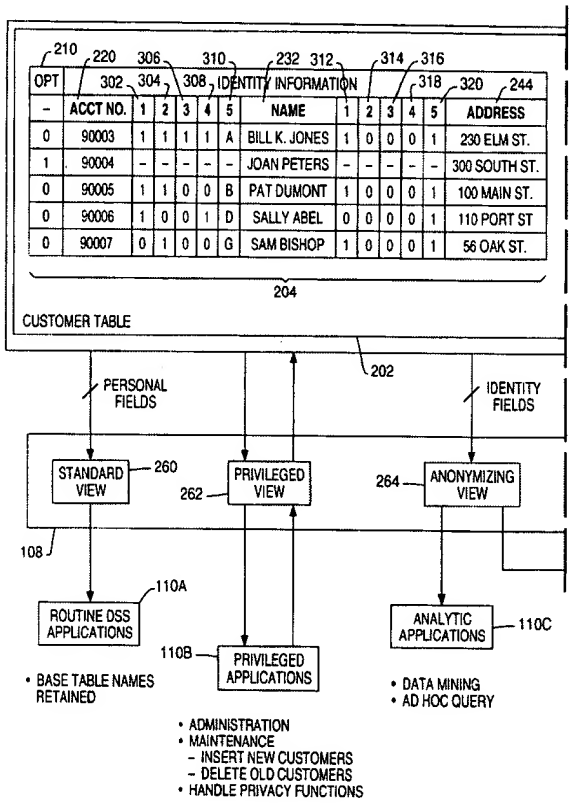
In the Figures, O'Flaherty shows administration access to underlying information of clients in a customer table 202 (and its attendant identity information portion 204, personal information portion 206, and sensitive information portion 208, for instance,) by way of the unfettered privileged view 262 in Figures 2A and 3A. In comparison, the standard view 260 and the anonymizing view 264 block applications 110A and 110C from receiving privacy parameters in a client's personal and identity field, respectively. Of course, Figures 2A and 3A are portions of larger figures and require coupling with 2B and 3B, 3C, respectively, to show the entire view, but are segmented (as in the patent) for simplicity below.

FIG. 2A




| OPT | 1 | 2 | 3 | 4 | 5 | ACCT NO. | NAME | ADDRESS | PHONE |
|---|---|---|---|---|---|---|---|---|---|
| – | 1 | 2 | 3 | 4 | 5 | | | | |
| 0 | 1 | 1 | 1 | 1 | A | 90003 | BILL K. JONES | 230 ELM ST. | (451) 342 – 9167 |
| 1 | – | – | – | – | – | 90004 | JOAN PETERS | 300 SOUTH ST. | (340) 456 – 8976 |
| 0 | 1 | 1 | 0 | 0 | B | 90005 | PAT DUMONT | 100 MAIN ST. | (312) 786 – 9873 |
| 0 | 1 | 0 | 0 | 1 | D | 90006 | SALLY ABEL | 110 PORT ST | (562) 451 – 7846 |
| 0 | 0 | 1 | 0 | 0 | G | 90007 | SAM BISHOP | 56 OAK ST. | (876) 567 – 9128 |

FIG. 3A




| OPT | ACCT NO. | 1 | 2 | 3 | 4 | 5 | NAME | 1 | 2 | 3 | 4 | 5 | ADDRESS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| – | | | | | | | | | | | | | |
| 0 | 90003 | 1 | 1 | 1 | 1 | A | BILL K. JONES | 1 | 0 | 0 | 0 | 1 | 230 ELM ST. |
| 1 | 90004 | – | – | – | – | – | JOAN PETERS | – | – | – | – | – | 300 SOUTH ST. |
| 0 | 90005 | 1 | 1 | 0 | 0 | B | PAT DUMONT | 1 | 0 | 0 | 0 | 1 | 100 MAIN ST. |
| 0 | 90006 | 1 | 0 | 0 | 1 | D | SALLY ABEL | 0 | 0 | 0 | 0 | 1 | 110 PORT ST |
| 0 | 90007 | 0 | 1 | 0 | 0 | G | SAM BISHOP | 1 | 0 | 0 | 0 | 1 | 56 OAK ST. |

**B. Each independent claim 1, 90, and 98 requires "the exclusion" of the "system administrator" from the digital identities managed by end users in "profiles" in safes, in turn, in vaults.[1] O'Flaherty, in apposition, unequivocally gives system administrators unfettered access to underlying privacy information of clients. For at least this reason, anticipation under 35 U.S.C. 102(e) fails.**

Although variously worded, the instant invention requires profiles in safes in vaults, with access rights of the vaults extending to the system administrator. At the same time, access rights of the profiles extend to the users, at the exclusion of the administrator. Ultimately, the profiles are for sharing with other users (who also have profiles administered by themselves at the exclusion of the administrator).

From above, O'Flaherty's privileged view 262 **"permits viewing, analysis, and alteration of all information [in customer table 202]**." *Emphasis added, col. 8, ll. 46-47.* It occurs relative to privileged applications 110B, **"such as those required for administration and/or maintenance of the database** (e.g. for inserting new customers, deleting ex-customers, handling address changes), **and to those applications which handle privacy related functions (such as informing customers about personal information collected about them, changing/updating personal information, and applying 'Opt-in/Opt-out' controls)**." *Emphasis added, col. 8, ll. 48-55.* Similarly, *col. 4, ll. 15-18,*

[1] The language of each claim controls their actual scope, but the argument here is simplified for illustration. This argument also presumes the Examiner's finding of fact that "profiles" of digital identities of users in the present invention correspond to that which the Examiner characterizes as "user[s] or consumer[]s can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63." *2-21-07 Office Action, p. 3, 2nd ¶.* Arguments below will challenge certain of the Examiner's findings of fact.

teaches that "all accesses to data, ***(with the exception of data access for administrative purposes)*** is accomplished through dataviews." *Emphasis added.*

In other words, those who perform system administration and maintenance on the extended database 106, which stores privacy parameters of clients in table 202, have unchecked access to the underlying privacy information of the clients. This cannot then anticipate, or even sustain a prima facie position of anticipation, for claims requiring "exclusion" of system administrators.

It is a feature of the invention to exclude system administrators, regardless of which system they administer, so users have complete control of their profiles. Appreciating system administrators need control over their computing domain, for maintenance or other functions, they are given control in the present invention by managing vaults, which house the safes of profiles of digital identities of users. In other words, the claims of the present invention impose a definitive barrier between profiles of users and the administrators, whereas the cited art does not. It adds a level of complexity not present in the prior art and, for at least this reason, foils anticipation.

As the law provides, a claimed invention is anticipated under 35 U.S.C. § 102 when all of the elements of the claimed invention are found in one reference. *See Scripps Clinic & Research Found. V. Genentech Inc.,* 927 F.2d 1565, 1576, 18 USPQ2d 1001, 1010 (Fed. Cir. 1991). Also, the prior art reference must disclose every limitation of the claimed invention, either explicitly or inherently. *In re Schreiber,* 128 F.3d 1473, 1477, 44 USPQ2d 1429, 1433 (Fed. Cir. 1997).

**C. Each independent claim 1, 90, and 98 requires users to have "exclusive" "access" and/or "administration" of their "profiles" of digital identities**

**in safes, in turn, in vaults.[2] O'Flaherty's giving system administrators access to underlying privacy information of clients destroys the required exclusivity that the user's have with their profiles, in safes, in vaults. For at least this reason, anticipation under 35 U.S.C. 102(e) fails.**

Again, O'Flaherty's privileged view 262 **"permits viewing, analysis, and alteration of all information [in customer table 202]."** *Emphasis added, col. 8, ll. 46-47.* It occurs relative to privileged applications 110B, **"such as those required for administration and/or maintenance of the database** (e.g. for inserting new customers, deleting ex-customers, handling address changes), and to those applications which handle privacy related functions (such as informing customers about personal information collected about them, changing/updating personal information, and applying 'Opt-in/Opt-out' controls)." *Emphasis added, col. 8, ll. 48-55.*

In other words, those who perform system administration and maintenance on the extended database 106, which stores privacy parameters of clients in table 202, have unchecked access to the underlying privacy information of the clients. This cannot then anticipate, or even sustain a prima facie position of anticipation, for claims requiring access rights of "profiles" of digital identities being given "exclusively" to users. O'Flaherty's granting "viewing, analysis, and alteration of all information" (*col. 8, ll. 46-47*) to administrators or other privileged users makes the user profiles non-exclusive, in apposition to the claims.

For at least this reason, the claims define themselves over the art.

---

[2] The language of each claim controls their actual scope, but the argument here is simplified for illustration.

**D. O'Flaherty never teaches anything other than unfettered access of administrators to the underlying privacy parameters of clients. As a result, O'Flaherty has no basis, much less a reasonable basis, for anticipating the independent claims 1, 90, and 98 requiring "exclusion" of the system administrator from "profiles" of digital identities of users or to the "exclusivity" in access granted to the users in their own profiles.[3]**

Appreciating many embodiments exist in a single patent, O'Flaherty teaches many forms of computing environments in which skilled artisans can practice O'Flaherty's invention. However, no embodiment exists relative to system administration and maintenance other than the one in which administrators have complete access and manipulation rights in the privacy parameters of clients in customer table 202. The reason this exists is so that administrators can handle the privacy functions related to sensitive user information. *See, Figures 2A and 3A, "HANDLE PRIVACY FUNCTIONS."* In contrast, the present invention relies not on administrators for privacy functions, but users for privacy, and by putting profiles in safe, that administrators cannot access, privacy is handled. In that administrators of the present invention can handles the safes in the vaults, but not the safe contents, administrators still have their information technology (IT) role fulfilled in the computing environment, which is vastly different than O'Flaherty.

Moreover, system administrators of O'Flaherty are not excluded from client identities and the mere granting of administrative rights to the client identities destroys the requirement of exclusivity being granted to users, as in the present invention. While subtle, the point should not be missed that access rights of underlying information of clients being granted to

[3] The language of each claim controls their actual scope, but the argument here is simplified for illustration.

system administrators, or other privileged users, in O'Flaherty makes for two reasons why the claims cannot be anticipated. First, the claims require that administrators are "excluded" from the digital identities of user profiles. Second, the claims require the users to have "exclusive" access rights to their profiles, regardless of excluding the administrators.

For at least this reason, anticipation fails.

**E. In the Examiner's rejection, no finding of fact ever establishes O'Flaherty as 1) "excluding" system administrators from having access to underlying information of user profiles in safes, in vaults, or 2) to users having "exclusive" access to their profiles. Thus, the Examiner has not made a *prima facie* anticipation rejection under 35 U.S.C. §102(e) relative to independent claims 1, 90, or 98, for at least two reasons. To the extent a *prima face* case has been made, though the Appellant disputes this, the below satisfactorily rebuts it.**

In fashioning his rejections, the Examiner appears to quote claim language from the present invention and points, parenthetically, to O'Flaherty where he thinks such is found. Such, however, is conspicuously missing in the teaching relative to the independent claims.

**Claim 1:** The Examiner rejects the claim limitation "and ***administered exclusively*** by a single one of the multiple users ***at the exclusion*** of the system administrator" according to the finding of fact "(i.e., user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63)." *Emphasis added, 2-21-07 Office Action, p. 3, 2nd ¶.*

While the Appellant does not dispute that users or consumers of O'Flaherty can access and change or update their privacy parameters, as the Examiner finds, no mention whatsoever

is made to the "exclusivity" of the users to their information or the "exclusion" of the system administrator from the information. Perhaps the Examiner does not making a finding of fact on this point because none exists. For at least this reason, the findings of fact are submitted as erroneous.

**Claim 90:** The Examiner rejects the claim limitation "the one or more safes of digital identities having multiple profiles ... ***each with access rights granted exclusively to the end users*** via the one or more accounts" according to the finding of fact "(i.e., 154, security information provides in fig. 2A access control rule for each user, col. 5, lines 29-63, col. 10, lines 27-64)." *Emphasis added, 2-21-07 Office Action, p. 11, ll. 2-6.* Also, the claim limitation "including ***the exclusion*** of access rights of the one or more system administrators" is rejected by the Examiner according to the finding of fact "(by each user without system administrators, col 8, lines 45-61)." *Emphasis added, 2-21-07 Office Action, p. 11, ll. 6-8.*

Upon a close inspection of the passages cited by the Examiner, however, none establishes that which the Examiners suggests they do. Rather, the cite to O'Flaherty at *col. 8, ll. 45-61*, especially in conjunction with Figures 2A and 3A, unequivocally establishes that system administrators have access to underlying privacy parameters of clients, not exclusion.

In relevant part, O'Flaherty insists that: "[t]he privileged view 262 **permits viewing, analysis, and alteration of all information [in customer table 202]**." *Emphasis added, col. 8, ll. 46-47.* It occurs relative to privileged applications 110B, **"such as those required for administration and/or maintenance of the database** (e.g. for inserting new customers, deleting ex-customers, handling address changes), and to those applications which handle privacy related functions (such as informing customers about personal information collected about them, changing/updating personal information, and applying 'Opt-in/Opt-out' controls)."

Not only does this access to information by system administrators destroy the Examiner's position that system administrators are "excluded," but the Examiner's position that O'Flaherty teaches user "exclusivity" to their privacy parameters is also destroyed.

Moreover, the foregoing quote of O'Flaherty is seen as giving system administrators the ability to "chang[e]/updat[e] personal information" and to "appl[y] 'Opt-in/Opt-out' controls." *Id.* In turn, this exactly contradicts the Examiner's finding of fact that "(each user (not administrator) can change privacy preference, col. 8, lines 45-61)." *2-21-07 Office Action, p. 13, ll. 6-7.* In other words, O'Flaherty expressly gives the system administrator the ability to change opt-in/opt-out controls which sets privacy preferences. In turn, the Examiner's reasoning is submitted as flawed.

For at least these reasons, the findings of fact are submitted as erroneous.

**Claim 98:** The Examiner rejects the notion of "the one or more safes of digital identities having multiple profile [sic] ... each with access right [sic] ***granted exclusively*** to the end users at location [sic] remote" according to the finding of fact "i.e., different data view for each user's privileged in fig. 2A-C, col. 8, lines 10-67 to col. 9, lines 64)." *2-21-07 Office Action, p. 13, ll. 2-5.* Also, the rejection includes "the multiple profiles ... being shared amongst the end users ***at the exclusion*** of the one or more system administrators (i.e., identity information can be accessed and shared by anonymizing view for any user (not administrator) in fig. 2A, col. 7, lines 10-67 to col. 8, lines 1-67 to col. 9, lines 1-63)." *Emphasis added, 2-21-07 Office Action, p. 13, ll. 7-11.*

First, the rejection above is not phrased as the claim is drafted and so any finding of fact based on the above is certainly less than accurate. The scope of the claim is only defined by the manner in which presented.

Second, the Examiner suggest that "exclusivity" per each user to privacy parameters in O'Flaherty exists because each user has access to their own information. While users may

indeed have access to their own privacy parameters, and while other users may not have access to the privacy parameters of other users (which may or may not exist in the O'Flaherty teaching), the fact that system administrators also have access to "all information" of users in the privileged view 262 (*col. 8, ll. 46-47*) destroys the requirement of user "exclusivity." For at least this reason, the findings of fact are submitted as erroneous.

Third, the Examiner suggests that because an anonymizing view 264 exists whereby users can share information, and such is seemingly without system administrator intervention, that anticipation is established. It is unreasonable, however, to sustain this rationale because system administrators in O'Flaherty are privileged users and have unfettered access to the privacy parameters of their client's in customer table 202, by way of a privileged view 262, not an anonymizing view. *See, also, col. 8, ll. 46-55.* Also, the anonymizing, standard and opt-out views are for "requestors" of privacy parameters of clients, such as third party applications 112 and business applications 110, not system administrators. As stated, "all accesses to data, ***(with the exception of data access for administrative purposes)*** is accomplished through dataviews." *Emphasis added, col. 4, ll. 15-18.*

For at least this additional reason, the findings of fact are submitted as erroneous.

**F. In the Examiner's rejection, no finding of fact ever establishes a "safe" as required in each of claims 1, 90 and 98. Thus, the Examiner has not made a *prima facie* anticipation rejection of independent claims 1, 90, or 98 under 35 U.S.C. §102(e). To the extent a *prima face* case has been made, though the Appellant disputes it, the below satisfactorily rebuts it.**

**Claim 1:** The Examiner finds that the extended database 106 of O'Flaherty is a corresponding "vault" in the instant invention. *2-21-07 Office Action, p. 3, l. 4-5.* He then

finds that "the vault for storing of multiple user objects for multiple users" is "(i.e., 202, customer table in fig. 2)." *2-21-07 Office Action, p. 3, l. 5-6.* Further on, the "safe object containing multiple different profiles" is "(fig. 2, col. 7, lines 10-67 to col. 8, lines 1-61)." *2-21-07 Office Action, p. 3, l. 11-12.* In that it seems reasonable to equate O'Flaherty's privacy parameters of multiple users in customer table 202 as a finding of fact for digital identity profiles of users, where then is the safe that keeps the profiles (as in claim 1 of the present invention)? In other words, if the "extended database 106 comprises a customer table 202," *col. 7, ll. 12-13*, and such equates to the claimed "vault" and digital identity "profiles," where then is the intervening structure, e.g., "the safe," in the vault, that stores the profiles? In still other words, O'Flaherty appears to provide two structures, e.g., the extended database 106 and the customer table 202, but such cannot equate to the claimed three structures, e.g., the vault, the safe (in the vault), and the digital identity profiles (in the safe, in the vault).

Alternatively, if the Examiner is suggesting the claimed vault is found in O'Flaherty as the extended database 106, the digital identity profiles are found as individual bits of user information, such as "Bill K. Jones, 230 Elm St...," *O'Flaherty, Figure 2A*, and O'Flaherty's customer table 202 corresponds to the claimed safe object, where then is the claimed "user object?"

In the Appellant's Specification, a "user object" is representatively seen as "Jane 308," in turn, storing one or more digital identity profiles 300, e.g., "My Hobby Profile," "My Biking," etc. For a given profile, it "can contain [still] other profiles, e.g., Profiles 302, 304, 306" and, "for a given user[,] may contain distinct pieces of identity data, or they may share certain pieces of data, e.g., a user's work phone number." *Appellant's Specification, p. 13, ll. 15-19.* In turn, "the single user's data is stored in a 'Safe' and multiples Safes are kept in a 'Vault.' This relationship between Safes 200 and a Vault 202 is illustrated in Figure 2." *Appellant's Specification, p. 13, ll. 10-11.* Alternatively phrased, safes and vaults are safe

objects and vault objects. In the claims, this is seen as "a vault for storage of multiple user objects" with "each of the user objects having a corresponding safe object."

The Examiner, however, never makes any appropriate finding of fact per each user object having a corresponding safe object. Rather, the Examiner points to the claimed limitation as a finding of fact in O'Flaherty as "(i.e., each profile object for personal identity information in customer table 202 in fig. 2, is restricted for accessing by such as, standard view, privileged view or anonymizing view, col. 7, lines 10-67 to col. 8, lines 1-61)." *2-21-07 Office Action, p. 3, ll. 9-11.* While certain privacy parameters of O'Flaherty are indeed restricted from view, according to particular views, this finding of fact points to restrictions on what third party or business applications 112 or 110 are entitled to. It is not reasonably related to each user object having a corresponding safe object as in the present invention.

For at least these reasons, the findings of fact are submitted as erroneous.

**Claims 90 and 98:** The Examiner finds "the one or more safes of digital identities having multiple profile [sic]" corresponds to a finding of fact "(i.e., identity information in fig. 2A)." *2-21-07 Office Action, p. 11, ll. 2-3 and p. 13, ll. 2-3.* If the Examiner equates O'Flaherty's identity information in fig. 2A as the digital identities having multiple profiles, no other cite is given by the Examiner showing correspondence to "the one or more safes." Alternatively, if the one or more safes corresponds to "the identity information in fig. 2A," where then is the finding of fact for the digital identities having multiple profiles? In either event, no rationale is provided. A finding of fact is missing for either 1) the safes or 2) the profiles and, for at least this reason, the finding of fact is erroneous.

Ultimately, the Appellant submits that anticipation is not established under any section of 35 U.S.C. §102.

**G. The Examiner's Finding of Fact in Claim 1 keeps repeating the same**

**O'Flaherty teaching for multiple, diverse propositions in the claims. For at least this reason, a *prima facie* anticipation rejection under any section of 35 U.S.C. §102 cannot be established.**

From the *2-21-07 Office Action at p. 3, l. 14 to p. 4, l. 4*, at four separate instances, the Examiner cites O'Flaherty as "(i.e., user or consumer can access and change or update profile information, col. 8, lines 46-67 to col. 9, lines 1-63)." However, this is applied as a finding of fact for each of:

1) and administered exclusively by a single one of the multiple users at the exclusion of the system administrator;

2) each profile including digital identity information provided by the single one of the multiple users;

3) and operable to be shared with other of the multiple users having other multiple different profiles accessible;

4) and administered exclusively by the other of the multiple users, the sharing occurring exclusively upon initiation by the single one of the multiple users.

While the Appellant does not dispute that users or consumers of O'Flaherty can access and change or update their privacy parameters, nowhere does the finding of fact establish the four claim limitations at hand.

For at least this reason, the findings of fact are submitted as erroneous.

**H. It is a feature of Claim 1 that the "sharing" of profiles of multiple users occurs "exclusively upon initiation by the single one of the multiple users." O'Flaherty's sharing of privacy parameters, however, occurs upon the**

**request of a third party application 112 or a business application 110. O'Flaherty cannot then anticipate under 35 U.S.C. §102(e).**

In claim 1, "operab[ility] to be shared" with others is a structural limitation of "each profile" of a user's digital identity information. A further limitation on the "sharing," however, is that it occur "exclusively upon initiation by the single one of the multiple users." In other words, the user who "owns" the digital identity profile, so to speak, is the party, and only party, that can initiate the sharing of their digital identity. In turn, this prevents third parties from seeking-out information of users that is not desired to be shared with them. In still other words, users themselves control who gets and who does not get their digital identities.

O'Flaherty, in contrast, has privacy parameters of clients in a repository customer table 202 that third party applications 112 and business applications 110 get simply by requesting it in the database management environment 100. For instance, step 508 of Figure 5 teaches "PROVIDE ACCESS TO THE DATA TO A REQUESTING ENTITY SOLELY THROUGH A DATABASE MANAGEMENT SYSTEM INTERFACE IN ACCORDANCE WITH THE PERSONAL PRIVACY PARAMETERS." To the extent users or clients of O'Flaherty desire to know information about the "requestors" of their data, one or more logging functions 510 and auditing roles 120 are contemplated. It is never the situation that O'Flaherty requires its clients to "exclusively initiate the sharing" of privacy parameters, as present claims 1 and 3-58 do.

For at least this reason, the anticipation rejection fails.

**I. Claims 90 and 98, and their progeny, are not anticipated under 35 U.S.C. §102(e) by O'Flaherty. O'Flaherty has no abstraction layers defining a vault, such as an identity server layer, an access protocol layer and an**

**identity manager layer, much less a vault defined by these layers for storing safes, in turn, for storing profiles with access to manage the vault extending to a system administrator while access and administration rights of the profiles are extended to users at the exclusion of the system administrator.**

In independent claims 90 and 98, a vault includes various software abstraction layers, such as "an access protocol layer, an identity server and an identity manager layer." The Examiner rejects the claims, however, by making associations to O'Flaherty that are internally inconsistent with other findings of fact. For example, the Examiner finds that the vault of claim 1 is equivalent to the extended database 106 of O'Flaherty's Figure 1. In claims 90 and 98, however, the "access protocol layer" of the vault is found to correspond to O'Flaherty's element 150 - "(i.e., 150 in fig. 1, privacy service to control data access in fig. 1, col. 5, lines 29-63)." *2-21-07 Office Action, p. 10, ll. 16-17 and p. 12, ll. 15-16.* From earlier in the rejection, the vault for storing safes of digital identities is found by the Examiner as "(i.e., identity field includes security information (154 in fig. 2B, fig. 1) in fig. 2A-B, col. 7, lines 10-65." *2-21-07 Office Action, p. 10, ll. 14-15 and p. 12, ll. 12-13.* As is clear, the Examiner tries to find facts associating the claimed vault as both an extended database 106 relative to claims 1 and 3-58 and, relative to claims 90 and 98, as structures associated with O'Flaherty's elements 150 and/or 154.

To the extent the Examiner is suggesting the vault is found in O'Flaherty as the extended database 106, then citing to elements 150 and/or 154 for the various layers defining the vault fails the anticipation rejection for elements 150 and 154 are not a part of the extended database 106, much less abstraction layers that define it.

On the other hand, if the Examiner is suggesting the vault is found in O'Flaherty as the privacy proxy service 150 and/or security information 154, then nowhere is there a

structure associated with 150, 154 that stores digital identity profiles, much less digital identity profiles in safes, in turn, in the vaults.

The Examiner further finds facts of the claimed "identity manager layer" of the vault as "(col. 4, lines 8-60)." *2-21-07 Office Action, p. 10, l. 18 and p. 12, l. 17.* At the cite given by the Examiner, O'Flaherty teaches many things, not the least of which includes, virtual databases, a data warehouse 102, dataviews 108, an extended database 106, business and third party applications 110, 112, and limiting access to privacy parameters according to the dataviews. What exactly then is the claimed "identity manager layer" in the fact finding that serves to define, in part, the vault of the present invention? At a minimum, the record is confusing. At worst, the record is a block cite to enormous amounts of teachings in hopes of having something correspond to the Appellant's claim limitations. In either, the record is not advanced by this type of rejection. Also, the record does not and cannot rise to the level of appropriate *prima facie* case of anticipation.

What appears to be happening is an Examiner oversimplifying the claim limitations. That is, the Examiner seems to hodgepodge together any element that teaches access, any element that teaches identities, and any element that teaches security and then concludes anticipation of the claims in view thereof. However, the instant invention is a precise arrangement of elements that is not found in the Examiner's mishmash of elements. Namely, claims 90 and 98 require an interaction that the three layers together, e.g., the access protocol, the identity server and the identity manager, define the vault that stores the profiles of users, wherein the vault has access rights granted to a system administrator while the profiles have rights that exclude the system administrator. For at least these additional reasons, the claims are patentable over O'Flaherty.

## J. Conclusion

The Appellant submits that (1) all claims are in a condition for allowance; (2) that O'Flaherty does not anticipate; and (3) the findings of fact are in serious question, thereby failing, at a minimum, the Examiner's burden of establishing a prima facie rejection. Accordingly, it is respectfully requested that the rejections of the pending claims be reversed and the application be remanded to the Examiner for allowance.

To the extent any fees are due beyond those authorized in the originally filed fee transmittal for filing a Notice of Appeal and brief in support thereof under 37 C.F.R. §§41.20(b)(1) and (b)(2), the undersigned again authorizes their deduction from Deposit Account No. 11-0978.

Respectfully submitted,

**KING & SCHICKLI, PLLC**

Michael T. Sanderson
Reg. No. 43,082

247 North Broadway
Lexington, KY 40507
(859) 252-0889

Certificate of Mailing

I hereby certify that this correspondence having 45 total pages is being deposited with the United States Postal Service as first class postage pre-paid mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on April 19 2007

Date 4/10/07 by

## VIII. CLAIMS APPENDIX

The claims on Appeal include 1, 3-58 and 90-101. Of those, claims 1, 20, 25, 49, 50, 58, 90, 98 and 101 appear as previously presented while all others remain as originally presented. Claims 2 and 59-89 remain canceled.

**The Listing of Claims:**

1. (Previously Presented) A computer server system for managing digital identity information, comprising at least one processor in operable connection with a memory configured by a database, the database including a vault for storage of multiple user objects for multiple users, the vault having access rights granted to a system administrator for management of the multiple user objects, each of the user objects having a corresponding safe object, the safe object containing multiple different profiles accessed and administered exclusively by a single one of the multiple users at the exclusion of the system administrator, each profile including digital identity information provided by the single one of the multiple users and operable to be shared with other of the multiple users having other multiple different profiles accessible and administered exclusively by the other of the multiple users, the sharing occurring exclusively upon initiation by the single one of the multiple users.

2. (Canceled)

3. (Original) The system of claim 1, wherein the safe object also contains at least one user-administered contact, each contact representing an entity outside the user's safe which receives controlled read access to digital identity information from at least one of the profiles.

4. (Original) The system of claim 1, wherein the safe object also contains at least one drop box object.

5. (Original) The system of claim 1, wherein the safe object also contains at least one application object with settings for an application.

6. (Original) The system of claim 1, wherein the safe object also contains at least one view object.

7. (Original) The system of claim 1, wherein the safe object also contains at least one access object.

8. (Original) The system of claim 1, wherein the system comprises a web server and an identity server.

9. (Original) The system of claim 8, wherein the web server and the identity server communicate using encrypted usernames.

10. (Original) The system of claim 8, wherein the web server and the identity server are secured by a firewall.

11. (Original) The system of claim 1, wherein the system comprises an identity server appliance.

12. (Original) The system of claim 1, further comprising a zero-byte client.

13. (Original) The system of claim 1, further comprising an installed client.

14. (Original) The system of claim 1, wherein the system comprises a provider model for access to the database, and the provider model abstracts the details of a particular directory and storage protocol.

15. (Original) The system of claim 1, wherein the system comprises an abstract model for access to the database, and the abstract model offers a hierarchical storage system in a representation that includes a user, a container, and data.

16. (Original) The system of claim 1, wherein the system comprises a programmatic interface to identity items and operations that correspond generally to directory service objects.

17. (Original) The system of claim 1, wherein the database includes multiple safe objects contained in a vault object.

18. (Original) The system of claim 17, wherein the system includes at least two vault objects hosted on different servers, each vault object contains at least one user safe object, and objects contained by the safe objects are federated to provide controlled access between the vault servers.

19. (Original) The system of claim 18, wherein the objects are federated using a Universal Resource Identifier which specifies at least a protocol, a host, a path, and an object.

20. (Previously Presented) The system of claim 1, further comprising a digital business card application object having a corresponding profile object which includes digital identity information provided by the single one of the multiple users.

21. (Original) The system of claim 1, wherein the system comprises a means for one user to receive updated profile information of another user using a link to the database.

22. (Original) The system of claim 1, wherein the database is a partitioned directory services database.

23. (Original) The system of claim 1, wherein the system is further characterized in that it provides an account creation service which creates a new account for a user based on a template.

24. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe management service which provides an administrative tool to manage and maintain safe objects.

25. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it provides a schema management service which permits the system administrator to at least view a directory service schema.

26. (Original) The system of claim 1, wherein the system is further characterized in that it provides a batch account creation service which creates several accounts at one time.

27. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which permits one to install and configure an identity server.

28. (Original) The system of claim 1, wherein the system is further characterized in that it provides a backup and restore service which allows one to backup and restore at least one safe object.

29. (Original) The system of claim 1, wherein the system is further characterized in that it provides a safe advisor service which allows one to verify the integrity of a safe object.

30. (Original) The system of claim 1, wherein the system is further characterized in that it provides a legal recovery tool which recovers digital identity information for forensic use.

31. (Original) The system of claim 1, wherein the system is further characterized in that it provides a data denormalization service which facilitates data transformation on database fields.

32. (Original) The system of claim 1, wherein the system is further characterized in that it provides a rules service.

33. (Original) The system of claim 1, wherein the system is further characterized in that it provides an event service which allows an identity server to register interest in and be notified of changes in the database.

34. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity verification service which allows one to verify the identity of a user based on registration information.

35. (Original) The system of claim 1, wherein the system is further characterized in that it provides an authorization service which allows a process to verify information gathered from a user registration form.

36. (Original) The system of claim 1, wherein the system is further characterized in that it provides a profile discovery and publishing service which allows users to publish at least a portion of their profile information.

37. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form fill-in service which allows a user to have the service fill in at least part of an online form with information from one of the user's profile objects.

38. (Original) The system of claim 1, wherein the system is further characterized in that it provides a form conversion service which assists a webmaster in converting existing forms to standardized field names.

39. (Original) The system of claim 1, wherein the system is further characterized in that it provides an install service which installs servlets on a web server.

40. (Original) The system of claim 1, wherein the system is further characterized in that it provides an identity exchange service for portions of a privacy protection protocol.

41. (Original) The system of claim 1, wherein the system is further characterized in that it provides a chat service which sets up chat rooms so users can communicate with each other in real time.

42. (Original) The system of claim 1, wherein the system is further characterized in that it provides a presence service which lets users specify where they are and allows them to discover another user's presence information.

43. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous remailer service which allows users to choose different email addresses for different profiles.

44. (Original) The system of claim 1, wherein the system is further characterized in that it provides an anonymous browsing service which allows a user to browse a network in an anonymous fashion to prevent sites from collecting user identity information.

45. (Original) The system of claim 1, wherein the system is further characterized in that it provides an infomediary service which facilitates creating an infomediary.

46. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and software for tracking IP addresses in order to selectively publish the last known IP address of a user.

47. (Original) The system of claim 1, wherein the system is further characterized in that it uses profile objects and at least one of an underlying directory service and an underlying file system in order to enforce access controls on web pages published by users.

48. (Original) The system of claim 1, wherein the system is further characterized in that it provides email services.

49. (Previously Presented) The system of claim 48, wherein the single one of the multiple users has an email address, and the system encodes contact relationship information in the email address.

50. (Previously Presented) The system of claim 48, wherein the system uses profiles to filter email sent to the single one of the multiple users.

51. (Original) The system of claim 1, further comprising a means for determining whether a user logging in at a third party web site is registered as a user of the system.

52. (Original) The system of claim 51, further comprising a means for logging the user into the system if the user is registered, and a means for registering the user and logging the user in if the user was not registered.

53. (Original) The system of claim 52, wherein the means for registering the user and logging the user in comprises a means for capturing user login information for the third party web site.

54. (Original) The system of claim 1, wherein the system is further characterized in that user digital identity information is only made available to a partner site if the user has flagged the information as public.

55. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a transaction history.

56. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a user authentication mechanism.

57. (Original) The system of claim 1, wherein the system is further characterized in that it uses an embossed icon which provides a launch point for launching application programs.

58. (Previously Presented) The system of claim 1, wherein the system is further characterized in that it uses a non-repudiation feature whereby the system administrator cannot change a user password and then log on as the user.

Claims 59-89 (Canceled)

90. (Previously Presented) A computer server system for managing digital identity information, comprising one or more processors in operable connection with one or more memories defining a vault for storage of one or more safes of digital identities, the vault including an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to one or more system administrators including management of the one or more safes of digital identities of one or more accounts of end users, the one or more safes of digital identities having multiple profiles each with access rights granted exclusively to the end users via the one or more accounts including the exclusion of access rights of the one or more system administrators, the multiple profiles being shared amongst the end users at the exclusion of the one or more system administrators.

91. (Original) The system of claim 90, wherein the access protocol layer includes one or more protocols selected from LDAP, XML, RPC-over-HTTP, XDAP or SMTP.

92. (Original) The system of claim 90, wherein the identity server layer serves as an NDS access point.

93. (Original) The system of claim 90, wherein the identity server layer maintains access rights to the digital identities.

94. (Original) The system of claim 90, wherein the identity manager layer includes NDS authentication and authorization that controls access to the digital identities.

95. (Original) The system of claim 90, wherein the identity manager layer has a secret store.

96. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are located on an identity server.

97. (Original) The system of claim 90, wherein the one or more processors and the one or more memories are functionally apportioned between a client, a web server and an identity server, including servlets and applets.

98. (Previously Presented) A configured computer-readable storage medium that manages digital identities, comprising a vault for secure storage of one or more safes of digital identity profiles, the vault having an access protocol layer, an identity server layer and an identity manager layer and having access rights granted to a system administrator for management of the safes of digital identity profiles, the one or more safes of digital identity profiles having access rights granted exclusively to one or more end users at locations remote from the vault, the one or more safes of digital identity profiles further including multiple profiles shared amongst the end users at the exclusion of the system administrator.

99. (Original) The configured storage medium of claim 98, further including a zero-byte client interface.

100. (Original) The configured storage medium of claim 98, further including a client application interface.

101. (Previously Presented) The configured storage medium of claim 98, further including a database including a user object and a corresponding safe object, the safe object containing at least one profile of the digital identity profiles.

# IX. EVIDENCE APPENDIX

None

## X. RELATED PROCEEDINGS APPENDIX

None